



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

7 October 2004

MEMORANDUM FOR DISTRIBUTION

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL
YEAR 2005 EXPENDITURES

During Fiscal Year 2005, the focus of our information management/information technology (IM/IT) efforts will continue to be the creation of a joint, net-centric environment that delivers knowledge dominance to the Naval war fighting team. Soon, our strengthened capital planning processes will ensure that we invest only in projects that are aligned with the Department's strategic vision. To align current programming with our goal of a secure, interoperable architecture, providing web-enabled services and full dimensional protection, our IM/IT programs must conform to the following policies:

Application, Data and Portfolio Management

- Efficiency requires that the portfolio of software applications operated on the Department's enterprise networks be rationalized to eliminate wasteful duplication and promote interoperability. The portfolio must then be actively managed to ensure that it continues to represent the optimal mix of investments. A key element of effective knowledge sharing is the maintenance of authoritative databases that are available to enterprise users to serve multiple requirements. Therefore, all applications or databases that are to be developed or procured for use on the Navy Marine Corps Intranet (NMCI) must be registered in the Department of the Navy Application and Database Management System (DADMS) and approved by the appropriate Functional Area Manager (FAM). Applications listed in DADMS as FAM Disapproved or Allowed with Restrictions are required to have retirement or migration plans (including firm termination/migration date, estimated cost of termination/migration, and identification of funding currently programmed and budgeted for those systems) approved by the Department of the Navy Chief Information Officer (DON CIO), via the appropriate DON Deputy CIO. Funding requested for these systems should be focused on their retirement or migration (allowing sustainment until transition is complete). Additionally, NMCI seats may only be ordered with software applications listed in DADMS as FAM Approved or Allowed with Restrictions. The DADMS homepage may be found at <https://www.dadms.navy.mil>.
- Use of proprietary extensions to Extensible Markup Language (XML)-based specifications is counterproductive to our interoperability goals and is prohibited on DON IT systems (View DON XML policy in the Policy and Guidance section at <https://www.doncio.navy.mil>).

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL
YEAR 2005 EXPENDITURES

- The Navy has established an enterprise license agreement for Oracle database licenses and maintenance for Navy shore-based activities. The agreement is centrally funded, and covers all Navy active duty, Reserve and civilian shore-based billets and contractors who access Navy systems supporting shore-based operations. Activities covered by this agreement shall not enter into separate Oracle database agreements for licenses or maintenance. More information is provided in the DASN(ACQ) and DON CIO joint memorandum "Navy Shore-Based Oracle database Enterprise License Agreement" of 29 September 2004, available at <https://www.doncio.navy.mil>. Go to the Policy & Guidance page and search on "Oracle".
- Commercial software agreements in place with vendors of products approved for use on DON IT systems have been negotiated to leverage the Federal Government's purchasing power to obtain favorable pricing. All commercial software procurements must comply with Defense Acquisition Regulation Supplement (DFARS) Subpart 208.74; DoDD 5000.2, paragraph E4.2.7 and the provisions of the SmartBUY enterprise software licensing agreement. To view the reference, and for information on the Enterprise Software Initiative, see <http://www.don-imit.navy.mil/esj/>.

Smart Card Technology

- The Common Access Card (CAC) has been designated as the Department of Defense's (DoD) primary physical access badge and carrier of public key infrastructure (PKI) digital credentials. DON activities procuring physical access systems, card badging systems and other smart card technology must use the CAC as their primary means to gain physical access (except for highly sensitive areas, such as SCIFs) and logical access to unclassified websites and networks. DON activities considering procurement of smart card technology other than the CAC (e.g., contactless physical access transactions) must provide DON CIO approval of their initiatives and conform to smart card configuration management requirements. DON Smart Card-PKI policy is posted in the Policy and Guidance section at <https://www.doncio.navy.mil>. The DON CIO point of contact for other-than-CAC initiative approval is Mr. Don Hildebrand, (703) 602-6729, donald.hildebrand@navy.mil
- All desktop/laptop computers procured by DON activities for connection to unclassified network services/NIPRNET must include smart card readers compatible with the DoD CAC, and all commands must enable cryptographic logon as soon as the required infrastructure is in place. The ASN(RD&A) memorandum "Smart Card Reader Requirement" of 3 June 2003 may be viewed in the Policy and Guidance section at <https://www.doncio.navy.mil>.

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL
YEAR 2005 EXPENDITURES

Ports, Protocols and Services (PPS)

- The DISN Security Accreditation Working Group (DSAWG) must approve PPS for all applications that are visible to DISA-managed network components.

Wireless Devices

- Wireless devices integrated with or connected to DoD networks are considered to be part of those networks. They must comply with DoDD 8500.1 and be certified and accredited per DoDI 5200.40.
- Authentication, non-repudiation, and personal identification in wireless devices must conform to DoD PKI guidance found in DoDD 8100.2 and DoDI 8520.2.

Privacy

- Per the E-Government Act of 2002, Section 208, DON activities must perform privacy impact statements (PIAs) before developing or procuring IT systems that collect, maintain, or disseminate information in a personally identifiable form from or about the public. The E-Government Act may be viewed at http://www.cio.gov/documents/e_gov_act_2002.pdf.

Public Key Infrastructure

- DON IT systems must support digital signing of email messages to ensure data integrity and non-repudiation; encryption of email messages containing For Official Use Only (FOUO), Sensitive but Unclassified (SBU), or privacy information; certificate-based client authentication for private websites; and cryptographic based network logon.

Internet Protocol Version Six (IPv6)

- All assets being developed, procured or acquired for the Global Information Grid (GIG) must be IPv6 capable, and must be interoperable with IPv4 systems/capabilities. This explicitly includes all acquisitions that reach Milestone C after October 1, 2003. The current version of the Department of Defense Information Technology Standards Repository (DISR) (<http://disronline.disa.mil/VJTA/index.jsp>) reflects this requirement. DoD policy on IPv6 is stated in DoD CIO memorandums of 9 June 2003 and 29 September 2003 (viewable on <http://ipv6.disa.mil/>).

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL
YEAR 2005 EXPENDITURES

Questions concerning the requirements above or the Department's enterprise implementation efforts may be directed to Mike LeValley, DON CIO Investment Management and Implementation Planning Team Lead, at (703) 602-6847.



D. M. Wennergren

Distribution:

CNO (N09B, N6, N61, N6F)
CMC (DCMS, C4)
CHNAVPERS
COMLANTFLT
COMPACFLT
COMNAVEUR
COMUSNAVCENT
COMSC
COMNAVRESFORCOM
COMNAVMETOCOM
COMNAVSECGRU
COMNAVNETWARCOM
BUMED
COMNAVAIRSYSCOM
COMSPAWARSYSCOM
COMNAVFACENGCOM
COMNAVSUPSYSCOM
COMNAVSEASYSYSCOM
ONI
NETC
NAVSTKAIRWARCEN
DIRSSP
COMNAVVSPECWARCOM
NCTSI
COMOPTEVFOR
COMNAVSYSMGTACT

Copy to:

Immediate Office of the Secretary (ASN(M&RA), ASN(I&E), ASN(RD&A),
ASN(FM&C) (FMO) (FMB-B)
GC
CNO (N82)